Chapter 42
Success Factors for Data Protection in Services and Support Roles: Combining Traditional Interviews With Delphi Method

Pedro Ruivo
Universidade Nova Lisboa, Portugal

Vitor Santos
Universidade Nova Lisboa, Portugal

Tiago Oliveira
Universidade Nova Lisboa, Portugal

ABSTRACT

The transformation of today's information and communications technology (ICT) firms requires the services and support organizations to think differently about customers data protection. Data protection represents one of the security and privacy areas considered to be the next "blue ocean" in leveraging the creation of business opportunities. Based in contemporary literature, the authors conducted a two phases' qualitative methodology - the expert's interviews and Delphi method to identify and rank 12 factors on which service and support professionals should follow in their daily tasks to ensure customer data protection: 1) Data classification, 2) Encryption, 3) Password protection, 4) Approved tools, 5) Access controls, 6) How many access data, 7) Testing data, 8) Geographic rules, 9) Data retention, 10) Data minimization, 11) Escalating issues, and 12) Readiness and training. This paper contribute to the growing body of knowledge of data protection filed. The authors provide directions for future work for practitioners and researchers.

DOI: 10.4018/978-1-5225-7113-1.ch042

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

Businesses and organizations are creating and using data at unprecedented rates. With this boom in data comes challenges and problems in data protection. Customers expect their data to be protected and not used in a manner inconsistent. The protection of their data is paramount to customers, and they evaluate information and communications technology (ICTs) firms in part on how well they handle and protect it from being stolen or used improperly. In many industries customers are specifically mandated to evaluate how ICTs firms protects their data. When customers create an account with ICTs firms, or use their services, they expect that a set of specific rules around how ICTs are used to manage their information (Cruz-Cunha & Portela, 2015). Previously, enterprises emphasized perimeter security over things like endpoint protection and data-centric security. If from one side the ever-expanding security and privacy perimeters make it necessary for companies to find data protection processes that secure data from both internal and external threats, placing the focus on sensitive data as it travels within and outside of enterprise networks. On the other side, the ever-changing landscape of data protection is not resulting in knowledge sharing and thoughts. With the sheer quantity of information and resources on data protection available today, it can be difficult to sort through it to find the most trusted and experienced sources that provide accurate insights and educated perspectives on relevant data protection challenges facing modern enterprises. In particular, the literature is lacking on methodological grounded knowledge about how ICT professionals should follow in order to ensure data protection. This is becoming critical as more and more ICT firms are evolving from a purely focus on software and communications to services providers, customer's data protection is critical factors in winning customer trust (Bélanger & Crossler, 2011; Pavlou, 2011; Slyke, Shim, Johnson, & Jiang, 2006; Stantcheva & Stantchev, 2014).

Reputable ICTs firms such as Microsoft, SAP, Portugal Telecom, ONI-Communications and Vodafone among others, have built a strong foundation of privacy and security practices (OECD, 2012). The past decade has brought immense changes in technology, requiring ICTs firms to continually evolve and reaffirm their commitment to trustworthy computing regardless if inshore, nearshore or offshore service and support models (Casado-Lumbreras, Colomo-Palacios, Ogwueleka, & Misra, 2014; Colomo-Palacios, Casado-Lumbreras, Soto-Acosta, Misra, & García-Peñalvo, 2012; Leeney, Varajão, Trigo Ribeiro & Colomo-Palacios, 2011). Hence is a must to continue to meet customer's data protection demands to meet regulations, customer expectations, and consumer perceptions (Hong & Thong, 2013; Pavlou, 2011). Instead of broadly study privacy or security situations handled by professionals this research paper focuses on the data protection field from the outlook of good practice in the management of IT human capital, filling a gap in the literature (Pavlou, 2011). Motivated by these issues, this study seeks to answer to the following research question:

RQ: What are the critical factors and their importance on which ICTs professionals in support and services roles should follow in their daily tasks in order to ensure customer's data protection?

To answer this question we developed and implemented a two phase's research: we commenced with the traditional questionnaires interview methodology with 17 experts in order to identify the factors, and then the Delphi method with 20 experts in order to obtain the ranking and consensus on the factors. The theoretical background is presented in the next section. Then we introduce the combined methodologies. After we present the results and analysis. Then the paper concludes with the main findings, including implications, limitations and future research opportunities.

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/success-factors-for-data-protection-in-services-and-support-roles/213834

Related Content

A Review on Application of Reinforcement Learning in Healthcare
Chitra A. Dhawaleand Kritika Anil Dhawale (2023). *Cyber Trafficking, Threat Behavior, and Malicious Activity Monitoring for Healthcare Organizations (pp. 105-119).*
www.irma-international.org/chapter/a-review-on-application-of-reinforcement-learning-in-healthcare/328128

Military Expenditure and Economic Growth Relationship Revisited in Some South Asian Countries: With Special Reference to India
Kanchan Datta (2019). *National Security: Breakthroughs in Research and Practice (pp. 810-835).*
www.irma-international.org/chapter/military-expenditure-and-economic-growth-relationship-revisited-in-some-south-asian-countries/220917

Critical Raw Materials and UK Defence Acquisition: The Case of Rare Earth Elements
Julieanna Powell-Turnerand Peter D. Antill (2019). *National Security: Breakthroughs in Research and Practice (pp. 673-693).*
www.irma-international.org/chapter/critical-raw-materials-and-uk-defence-acquisition/220908

Architecture of Combined E-Learning Environment and Investigation of Secure Access and Privacy Protection
Radi Petrov Romanskyand Irina Stancheva Noninska (2019). *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications (pp. 1347-1365).*
www.irma-international.org/chapter/architecture-of-combined-e-learning-environment-and-investigation-of-secure-access-and-privacy-protection/213858

The E-Government Surveillance in the United States: Public Opinion on Government Wiretapping Powers
Ramona Sue McNeal, Mary Schmeidaand Justin Holmes (2016). *Ethical Issues and Citizen Rights in the Era of Digital Government Surveillance (pp. 208-230).*
www.irma-international.org/chapter/the-e-government-surveillance-in-the-united-states/145569